UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,690	09/12/2003	David D. Brandt	03AB014B/ALBRP303USB	7383

7590 10/01/2008

Susan M. Donahue
Rockwell Automation, 704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
KIM, TAE K	
ART UNIT	**PAPER NUMBER**
2153	
MAIL DATE	**DELIVERY MODE**
10/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/661,690	BRANDT ET AL.	
	Examiner	Art Unit	
	TAE K. KIM	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 30 May 2008.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-5 and 9-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-5 and 9-29 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This is in response to the Applicant's response filed on May 30, 2008. Claims 6 – 8, 30, and 31 have been cancelled by the Applicant. Claims 1, 17, 20, 24, 25, and 28 have been amended. Claims 1 – 5 and 8 – 29, where Claims 1, 17, 20, 24, 25, and 28 are in independent form, are presented for examination.

Claim Rejections - 35 USC § 112

With regards to the Sec. 112, 1st paragraph rejections to Claims 1 – 5 and 8 – 16, the Applicant has amended the claims to properly reflect the capabilities of the claimed invention as supported by the specification. The Sec. 112 rejections are withdrawn.

Claim Rejections - 35 USC § 101

With regards to the Sec. 101 rejections to Claims 1 – 5, 8 – 16, and 24—27, the Applicant has amended the claims to include physical embodiments of the invention. The Sec. 101 rejections are withdrawn.

Claim Objections

Claim 21 is objected to because of the following informalities: "extended security protocol" is not disclosed in Claim 20, which Claim 21 depends on. "Extended" should be corrected to "heavyweight." Appropriate correction is required.

Claim 23 is objected to because of the following informalities: "path component" is not disclosed in Claim 20, which Claim 23 depends on. "Path component" should be corrected to " the session." Appropriate correction is required.

Response to Arguments

Applicant's arguments filed on May 30, 2008 have been fully considered but they are moot based on the new grounds of rejection as stated below.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1 – 5 and 9 - 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,760,782, invented by Andrew G. Swales (hereinafter "Swales"), in view of U.S. Patent 6,842,860, invented by Dennis K. Branstad et al. (hereinafter "Branstad").

1. Regarding Claims 1, 17, and 24, Swales discloses an automation security system and method [Fig. 4; Col. 2, lines 39-60; web server takes the role of a TCP/IP router to resolve security issues when users attempt to remotely interface with an industrial control system], comprising:

a plurality of automation assets [Fig. 4, items 70, 80, 84; Col. 2, lines 27-38; industrial control system that has a programmable logic control system with programmable logic controller with I/O devices];

a plurality of remote devices or networks that utilize a factory protocol to transport data between the plurality of automation assets and the plurality of remote devices or networks [Figs. 1 and 5; Col. 3, line 54 – Col. 4, line 31; one or more users can remotely access the process control system and the devices attached to the process control system (automation assets) on the network (using TCP/IP; factory protocol) via a website on a computer (remote devices)],

Swales further discloses the use of a unique internet address for the website that is utilized to access the process control monitoring system [Col. 4, lines 32-43].

Swales, however, does not specifically disclose that the factory protocol utilizes at least one security field to authenticate at least one of a requestor of the data and a supplier of the data, the security field provides at least one of a security parameter or a performance parameter, or that the factory protocol is dynamically changed or adjusted based upon considerations of desired security levels and real time communications performance and employs lightweight or heavyweight encryption mechanisms based on the performance parameter.

Branstad discloses the use of various levels of security authentication mechanisms depending on various system conditions regarding security authentication speeds with message authentication codes (used to authenticate sender or requestor of data) standard to security protocol IPSec (part of the Internet Protocol suite TCP/IP) [Fig. 3; Col. 3, Lines 43-49, 54-56; Col. 4, Lines 2-7, 53-61]. Branstad also discloses that the authentication system is designed to adaptively adjust its authentication strength and speed to meet current needs based on consideration such as security policy (desired security levels), observed authentication error rates, alarms from host or network defenses, and processor loading (real-time communication performance) [Col. 4, lines 2-7]. Branstad further discloses that for low-speed, high-strength communication within the network, the authentication system uses HMACs (heavyweight encryption mechanisms) and for high-speed, lower-strength

communication, the system uses PMAC (lightweight encryption) based on the needs of the observed system.

It would have been obvious to one skilled in the art to incorporate the teaching of Branstad in the Swales system since the Swales system utilizes TCP/IP to communicate with the industry control system. TCP/IP allows the use of the IPSec security protocol to secure communications within a communication network.

The motivation to combine, as disclosed in Branstad, is that the levels of security at one level may make network connections too slow to process real-time high-speed video [Col. 1, Lines 26-34] and that selectively authenticating data, as described above, is a method to remedy that issue.

2. Regarding Claim 2, Swales, in view of Branstad, discloses all the limitations of Claim 1 above. Swales further discloses that the security field further comprises path information to at least one of identify a requester/supplier of a connection, authenticate the requestor, and/or authenticate the supplier [Col. 4, lines 32-43; the use of a unique internet address for the website that is utilized to access the process control monitoring system via TCP/IP].

3. Regarding Claim 3, Swales, in view of Branstad, discloses all the limitations of Claim 2 above. Swales further discloses that the path information facilitates non-connected data access by sending out an open-ended message [Col. 4, lines 32-43; the use of a website allows non-connected data access using open-ended messages].

4. Regarding Claim 4, Swales, in view of Branstad, discloses all the limitations of Claim 1 above. Swales further discloses that the end points include at least one

automation asset, the automation asset includes at least one of an I/O device [Fig. 2, item 40].

5. Regarding Claim 5, Swales, in view of Branstad, discloses all the limitations of Claim 1 above. Swales further discloses that the network communications channel is established across at least one of a public network [Col. 4, lines 32-43; access is via a website on the Internet].

6. Regarding Claim 9, Swales, in view of Branstad, discloses all the limitations of Claim 1 above. Swales further discloses that the factory protocol including at least one of a message integrity component [Col. 4, lines 32-43; accessing the process control monitoring system via TCP/IP; inherent that TCP/IP uses checksum to determine integrity of data]

7. Regarding Claim 10, Swales, in view of Branstad, discloses all the limitations of Claim 1 above. Swales further discloses that the factory protocol is adapted to at least one of an object model that protects configuration of and transport of data between intelligent devices [Col. 4, lines 32-43; accessing the process control monitoring system via TCP/IP model].

8. Regarding Claim 11, Swales, in view of Branstad, discloses all the limitations of Claim 1 above. Swales further discloses of a component to perform check sum tests [Col. 4, lines 32-43; accessing the process control monitoring system via TCP/IP; inherent that TCP/IP uses checksum to determine integrity of data].

9. Regarding Claim 12, Swales, in view of Branstad, discloses all the limitations of Claim 1 above. Swales further discloses that the factory protocol facilitates at least one

of an identification to establish network trusts [Col. 4, lines 32-43; the use of a unique internet address for the website that is utilized to access the process control monitoring system via TCP/IP].

10. Regarding Claims 13, 14, 16, 18, and 19, Swales, in view of Branstad, discloses all the limitations of Claims 1 and 17 above. However, Swales nor Branstad specifically discloses that the factory protocol is associated with a protocol supporting at least one of a Temporal Key Interchange Protocol (TKIP) and a wireless protocol. Neither is the specific employment of an Elliptical function, an Aziz/Diffie Protocol, a Kerberos protocol, a Beller-Yacobi Protocol, an Extensible authentication protocol (EAP), an MSR+DH protocol, a Future Public Land Mobile Telecommunication Systems Wireless Protocols (FPLMTS), a Beller- Chang-Yacobi Protocol, a Diffie-Hellman Key Exchange, a Parks Protocol, an ASPECT Protocol, a TMN Protocol, RADIUS, Groupe Special Mobile (GSM) protocol, or a Cellular Digital Packet Data (CDPD) protocol with the system disclosed in the mentioned references. Neither Swales nor Branstad disclose the use of a security field to limit access based upon line of sight parameters.

It is commonly known to one of ordinary skill in the art that various wireless, including those using line of sight parameters, and communication protocols can be used within an automated factory network, such as CIP, TKIP, EAP, Aziz/Diffie Protocol, Kerberos protocol, Beller-Yacobi Protocol, MSR+DH protocol, FPLMTS, Beller-Chang-Yacobi Protocol, Diffie-Hellman Key Exchange, Parks Protocol, ASPECT Protocol, TMN Protocol, RADIUS, GSM protocol, and CDPD protocol. It would have been obvious to one skilled in the art at the time of the invention that a method of providing network

security, such as the one described in Swales or Branstad, would be adaptable and implemented on multiple network protocols that existed at that time. It would have also been obvious that a method of providing network security can "tunnel" through multiple types of networks that use such network protocol, such as the ones described above. Furthermore, the use of the various combinations of the aforementioned components for any communication and security protocol ensures proper transmission and authorized access of information across a network. The broad compatibility within networks and protocols available follows within the concept of allowing various components, which are more than likely to be manufactured by different vendors, to communicate seamlessly. Allowing access to the factory network wirelessly, virtually, or remotely improves the accessibility of the network and communications between an authorized user and component or between components.

11. Regarding Claim 15, Swales, in view of Branstad, discloses all the limitations of Claim 1 above. Swales further discloses that the network communications channel employs at least one of an Ethernet network [Col. 5, lines 13-18; TCP/IP network via Ethernet].

12. Regarding Claims 20 and 21, Swales discloses a method to facilitate automation network security establishing a communications session and exchanging data with an automation asset [Fig. 4; Col. 2, lines 39-60; web server takes the role of a TCP/IP router to resolve security issues when users attempt to remotely interface with an industrial control system]. Swales, however, does not specifically disclose of determining a need for real-time communication, establishing a communications

session via a heavyweight encryption mechanism if real-time communications is not needed, and exchanging data in accordance with real time communications via a lightweight encryption mechanism that induces minimal impact on a system's performance if real-time communication is needed.

Branstad discloses the use of various levels of security authentication mechanisms depending on various system conditions regarding security authentication speeds with message authentication codes (used to authenticate sender or requestor of data) standard to security protocol IPSec (part of the Internet Protocol suite TCP/IP) [Fig. 3; Col. 3, Lines 43-49, 54-56; Col. 4, Lines 2-7, 53-61]. Branstad also discloses that the authentication system is designed to adaptively adjust its authentication strength and speed to meet current needs based on consideration such as security policy (desired security levels), observed authentication error rates, alarms from host or network defenses, and processor loading (real-time communication performance) [Col. 4, lines 2-7]. Branstad further discloses that for low-speed, high-strength communication within the network, the authentication system uses HMACs (heavyweight encryption mechanisms) and for high-speed, lower-strength communication, the system uses PMAC (lightweight encryption) based on the needs of the observed system.

It would have been obvious to one skilled in the art to incorporate the teaching of Branstad in the Swales system since the Swales system utilizes TCP/IP to communicate with the industry control system. TCP/IP allows the use of the IPSec security protocol to secure communications within a communication network.

The motivation to combine, as disclosed in Branstad, is that the levels of security at one level may make network connections too slow to process real-time high-speed video [Col. 1, Lines 26-34] and that selectively authenticating data, as described above, is a method to remedy that issue.

13. Regarding Claim 22, Swales, in view of Branstad, discloses all the limitations of Claim 20 above. Branstad further discloses that the lightweight security protocol includes at least one of an encryption field [Col. 5, lines 17-22; high-speed, lower-strength mechanisms include partial message authentication codes (PMAC), which is a hash-based encryption system].

14. Regarding Claim 23, Swales, in view of Branstad, discloses all the limitations of Claim 20 above. Swales further discloses of a component to identify a requestor of data [Col. 4, lines 37-43; user list and associated password used to determine access to system].

Claims 25 - 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Swales, in view of Branstad, and further in view of "AI Techniques Applied to High Performance Computing Intrusion Detection" by Susan M. Bridges et al. (hereinafter referenced as "Bridges").

15. Regarding Claims 25—29, Swales discloses an automation security system and method [Fig. 4; Col. 2, lines 39-60; web server takes the role of a TCP/IP router to resolve security issues when users attempt to remotely interface with an industrial control system], comprising:

a plurality of automation assets [Fig. 4, items 70, 80, 84; Col. 2, lines 27-38; industrial control system that has a programmable logic control system with programmable logic controller with I/O devices];

a plurality of remote devices or networks that utilize a factory protocol to transport data between the plurality of automation assets and the plurality of remote devices or networks [Figs. 1 and 5; Col. 3, line 54 – Col. 4, line 31; one or more users can remotely access the process control system and the devices attached to the process control system (automation assets) on the network (using TCP/IP; factory protocol) via a website on a computer (remote devices)],

Swales further discloses the use of a unique internet address for the website that is utilized to access the process control monitoring system [Col. 4, lines 32-43].

Swales, however, does not specifically disclose that the factory protocol utilizes at least one security field to authenticate at least one of a requestor of the data and a supplier of the data, the security field provides at least one of a security parameter or a performance parameter, or that the factory protocol is dynamically changed or adjusted based upon considerations of desired security levels and real time communications performance and employs lightweight or heavyweight encryption mechanisms based on the performance parameter. Nor does Swales specifically disclose the utilization of an intrusion detection component or methodology.

Branstad discloses the use of various levels of security authentication mechanisms depending on various system conditions regarding security authentication speeds with message authentication codes (used to authenticate sender or requestor of

data) standard to security protocol IPSec (part of the Internet Protocol suite TCP/IP) [Fig. 3; Col. 3, Lines 43-49, 54-56; Col. 4, Lines 2-7, 53-61]. Branstad also discloses that the authentication system is designed to adaptively adjust its authentication strength and speed to meet current needs based on consideration such as security policy (desired security levels), observed authentication error rates, alarms from host or network defenses, and processor loading (real-time communication performance) [Col. 4, lines 2-7]. Branstad further discloses that for low-speed, high-strength communication within the network, the authentication system uses HMACs (heavyweight encryption mechanisms) and for high-speed, lower-strength communication, the system uses PMAC (lightweight encryption) based on the needs of the observed system.

It would have been obvious to one skilled in the art to incorporate the teaching of Branstad in the Swales system since the Swales system utilizes TCP/IP to communicate with the industry control system. TCP/IP allows the use of the IPSec security protocol to secure communications within a communication network.
The motivation to combine, as disclosed in Branstad, is that the levels of security at one level may make network connections too slow to process real-time high-speed video [Col. 1, Lines 26-34] and that selectively authenticating data, as described above, is a method to remedy that issue.

Branstad further discloses that the authentication system is designed to adaptively adjust its authentication strength and speed based on alarms from hosts

[Col. 4, lines 2-7]. Branstad, however, does not specifically disclose the utilization of an intrusion detection component or methodology to trigger those alarms.

Bridges discloses a system and method of using artificial intelligence within a high performance computer environment detect intrusions in the network. Specifically, Bridges discloses its use within a cluster computing architecture using both TCP/IP and Giganet networking protocols [pg. 1, paragraph 3]. The system combines both anomaly and misuse detection mechanisms and uses both network traffic and system audit date as inputs, meaning the intrusion detection is both host and network-based [pg. 1, paragraph 1]. Fuzzy logic is used with association rules and frequent episodes to "learn" normal patters of the system behavior. If certain events leave a set of patterns that are below a specified threshold, the system issues an alarm. The system can also implement rules that match patters of known attacks or patterns that are commonly associated with suspicious behavior to identify attacks [pg. 2, paragraph 5]. The system also uses a Decision Module determine the security actions once an attack is detected [pg. 9, paragraph 1]

It would have been obvious to one skilled in the art at the time of the invention to combine the teachings of Bridges with the automation security system in Swales by including the intrusion detection module in the web server that provides the website that accesses the automation system.

The motivation to do so is so the automation security system will monitor for intrusions and unauthorized access is necessary due to the possibility of address spoofs or tunneling into the network. The Bridges system particularly functions well in

an automated system where performance degradation is generally not acceptable. Furthermore, the ability of the Bridges system to use multiple communication protocols that are also usable in an automated security system makes the Bridges system very desirable as an intrusion detection system.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tae K. Kim, whose telephone number is (571) 270-1979. The examiner can normally be reached on Monday - Friday (8:00 AM - 5:00 PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton B. Burgess, can be reached on (571) 272-3949. The fax phone number for submitting all Official communications is (703) 872-9306. The fax phone number for submitting informal communications such as drafts, proposed amendments, etc., may be faxed directly to the examiner at (571) 270-2979.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866) 217-9197 (toll-free).

/Tae K. Kim/
9/28/08

/Liangche A. Wang/
Primary Examiner, Art Unit 2153